Exhibit E

RIDGEVIEW MEDICAL CENTER AND CLINICS #3501

SUBJECT: ACCESS CONTROL POLICY

ORIGINATING DEPT: MIS

DISTRIBUTION DEPTS: All

ACCREDITATION/REGULATORY STANDARDS:

Original Date: 12/12 **Revision Dates:** **Reviewed Dates:**	**APPROVAL:** Administration: _____ Director: _____

PURPOSE:

The purpose of the Ridgeview Medical Center Access Control Policy is to establish the requirements necessary to ensure that access to Ridgeview Medical Center Information Resources is managed in accordance with:

- Business requirements,
- Information security requirements, and;
- Other Ridgeview Medical Center policies and procedures

Ridgeview Medical Center follows a traditional role-based access control model.

Audience

The Ridgeview Medical Center Access Control Policy applies equally to all individuals who are responsible for managing Ridgeview Medical Center Information Resource access, and those granted access privileges to any Ridgeview Medical Center Information Resource.

POLICY:

- In general, all access to Ridgeview Medical Center Information Resources must be justified by a legitimate business requirement prior to approval.
- Ridgeview Medical Center Information Resources, including network devices, servers, and applications, must have a corresponding ownership responsibilities identified and documented.
- Information Resource owners are responsible for the approval of all access requests. (Reference: RMC Policy #3508 - *Data Classification*)
- User accounts and access rights for all Ridgeview Medical Center Information Resources must be reviewed and reconciled on no less than an annual basis.
- User account and access right reviews and actions must be documented.
- Creation of user accounts and access right modifications must be documented and/or logged.
- Only the level of access required to perform authorized tasks may be approved, following the concept of "least privilege".
- Account creation must follow a documented user registration process.
- Account must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- Whenever possible, access to Information Resources should not be granted directly to individual accounts.
- Whenever possible, shared accounts should not be used. Where shared accounts are used, their use must be documented and approved by the Information Resource owner.
- Upon user role changes, access rights must be modified in a timely manner to reflect the new role.

- Access to Confidential information is based on "need to know". (Reference: RMC Policy #3508 - *Data Classification*).
- Confidential data access must be logged.
- All users must sign the Ridgeview Medical Center Enterprise Information Security Governance Policy Acknowledgement before access is granted to an account or Ridgeview Medical Center Information Resources.
- Documented user access rights and privileges to Information Resources must be included in disaster recovery plans, whenever such data is not included in backups.
- All RMC external network access to confidential information requires access to include two factor authentication.
- Remote access to Information Resources may only be granted to individuals with a justifiable business need or requirement.
- Remote access requests must be approved by the requestor's manager or Ridgeview Medical Center IS Management.
- Remote access to Information Resources must be logged.
- Users granted remote access privileges must be given remote access instructions and responsibilities.

WAIVERS:

Waivers from certain policy provisions may be sought following the process outlined in the Ridgeview Medical Center Policy #3511 – *Enterprise Information Security Governance*.

ENFORCEMENT:

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights and termination of contract(s).

VERSION HISTORY OF SOURCE DOCUMENT: Ridgeview Medical Center Information Security Policy Manual

Version Number	Date	Reason/Comments
V1.00	December, 2012	Document Origination
V2.00	May, 2014	Full review with IT Steering Committee
V3.00	August, 2015	Reviewed with Security Committee
	6/16	Finalized, assigned policy number, on RidgeNet. Previous documentation not archived.